论数字时代侦查机关收集通信信息的法律规制

艾　明

摘　要：我国目前虽然已初步构建起规制侦查机关收集通信信息的法律体系，但这一体系未能较好地因应数字时代的发展趋势，存在诸多不足。在数字时代，多元化样态的通信信息背后承载着不同的保护法益。立法者应当区分这些不同的保护法益，依循通信信息类型的本质特征，作出合乎比例的、有针对性的法律规制。具体而言，我国应从如下方面加强法律规制：一是由刑事诉讼法为某些新型侦查措施提供特别授权依据，以符合宪法要求；二是按照通信信息类型的不同，以比例原则为指导进行相应密度的法律规制；三是大幅度提升扣押邮件、电报措施的法律规制密度；四是对查看嫌疑人手机通信内容信息的行为进行独立授权；五是建立符合《个人信息保护法》要求的相应保护机制。

关键词：数字时代；侦查机关；通信信息；个人信息；法律规制

中图分类号：D925.2　　**文献标识码：**A　　**文章编号：**1003-0751(2024)03-0055-09

数字时代的到来使通信信息的类型产生了裂变。受益于数字技术的发展，通信信息在产生、传输、存储中发生了巨大变化，衍生出许多新形态。例如，在产生端，除了生成通信内容信息外，亦会产生大量的通信记录信息。在传输端，除了通过电信运营商提供的设备传输通信内容信息外，还会借助即时通信软件传输通信内容信息。在存储端，大量的通信内容信息（如电子邮件）和通信记录信息被存储于第三方系统中。多元化样态的通信信息背后承载着不同的保护法益，立法者应根据保护法益的不同，制定合理的规制策略。

侦查领域是国家干预公民通信自由和通信秘密权的重要场域。为了平衡打击犯罪和保障公民权利之间的关系，立法者应当顺应数字时代的变化趋势，对侦查机关收集通信信息的行为作出合乎比例的、密度有别的明确规制。然而，我国现行立法并未积极因应数字时代通信信息类型的多元化趋势，进行有针对性的改进，实务中，因缺乏法律的清晰指引，屡生争议。常见的争议主要包括收集嫌疑人手机通话记录的侦查措施究竟属于技术侦查措施还是调取证据措施①，可以用于收集通信信息的网络在线提取措施和电子数据检查措施属于刑事诉讼法意义上何种类型的侦查措施[1]，扣押嫌疑人手机后侦查人员查看其手机存储的通信信息是否需要独立的法律授权[2]，等等。有鉴于此，笔者拟在分析数字时代通信信息多样化样态的基础上，探寻规制侦查机关收集通信信息措施的法律原理，并以此原理审视我国立法和司法现状，发现问题，最后提出完善建议。

一、数字时代通信信息的类型与规制原理

进入数字时代，通信信息的类型呈现出多元化

收稿日期：2023-09-15

基金项目：四川省智慧警务与国家安全风险治理重点实验室2023年度开放课题“智慧公安建设中数据型警察职权配置的法治路径研究”（ZHKFYB2306）。

作者简介：艾明，男，西南政法大学诉讼法与司法改革研究中心教授、博士生导师（重庆　401120），智慧警务与国家安全风险治理重点实验室研究员（四川泸州　646000）。

样态,每一种通信信息类型都承载着不同的保护法益。立法者应当区分这些不同的保护利益,依循通信信息类型的事物本质,作出合乎比例的、有针对性的法律规制。

(一)通信内容信息和非内容信息

按照《现代汉语词典》的释义,“通信”是指利用电波、光波等信号传送文字、图像等[3]。《中华人民共和国电信条例》第2条规定,“电信”是指利用有线、无线的电磁系统或者光电系统,传送、发射或者接收语音、文字、数据、图像以及其他任何形式信息的活动。美国《联邦电子通信隐私法》(The Electronic Communications Privacy Act,以下简称ECPA)将“电子通信”定义为:透过有线、无线、电磁或光电等方式所传送的符号、讯号、文字、图像、声音、资料或资讯。

根据以上定义,利用通信信号或通信系统传送的任何文字、图像或其他形式信息,属于通信内容信息。除此之外,在数字时代,通信过程还会产生大量的非内容信息。例如,在手机使用的过程中,每一次通话都会产生受话人号码、通话开始和结束的日期和时间、通话时长、通话所使用的手机基站信息(Cell-ID),这些非内容的通信记录信息被存储在电信服务商的运营系统中。非内容性的通信记录信息蕴藏着通话对象的社交关系、地理位置、行踪轨迹,对侦查具有重要价值,成为数字时代侦查机关收集运用的重要信息资源[4]。

总体而言,法律保留以及法益保护是在规制通信内容信息和通信记录信息的收集时最为重要的法律规制原理。

第一,通信内容信息和通信记录信息都属于公民通信自由和通信秘密基本权利的保护范围,因此,国家权力机关不论是收集通信内容信息还是收集通信记录信息,都应当遵守法律保留的原则,必须有明确的法律授权依据。

例如,在2003年的“电信通信记录”判决中,德国联邦宪法法院明确表示:“秘密通讯虽然主要在于保障通讯的内容,但同样地亦包括保障通讯的情况。属此等项目者,尤其是是否、何时,以及多常介于何人或机构间,发生或尝试建立通讯往来。对此,国家原则上亦不得试图加以探求。”②为了回应这一判决,德国在修改刑事诉讼法时,专门增订了第100g条,作为侦查机关收集电信通信记录信息的法律特别授权依据。又如,为了规制执法机关收集通信记录信息的行为,美国国会在ECPA中专门制定了《存储通信法》(The Stored Communications Act,简称SCA)和《笔式记录器法》(The Pen Registration Act)。

第二,在保护的法益方面,立法者一般认为,通信内容信息比非内容的通信记录信息承载了更重要的保护法益,因此,有必要对侦查机关收集通信内容信息的行为进行更高密度的法律规制。“制宪者希望给予最为严格标准保护的只是‘通信内容’,……而通话对象、通话时间、通话规律等‘非内容的通信信息’,固然属于通信秘密的保护范围,但受保护程度显然较通信内容为低。”[5]

针对侦查机关监听电信通信的行为,德国刑事诉讼法分别从证据门槛(一定的事实构成嫌疑)、适用的犯罪类型(明确列举的严重犯罪行为)、严格的审批手续(只能依检察官申请由法院签发命令)、法院命令记载的明确性要求、执行期限(最长期限为三个月)等方面进行了较高密度的法律规制。侦查机关新发展出的线上搜索的侦查措施,亦会收集公民利用互联网传送的通信内容信息。“如果计算机网络中连续通信的内容信息和状况信息被侦查人员截取,不管侦查人员是针对电信传输线路还是在终端设备采取技术措施,都不可避免地会干预秘密通讯之自由。”[6]2017年,德国修订刑事诉讼法时,专门增加了线上搜索的法律规定,对该侦查措施进行了高密度的法律规制[7]。与之相比,对于侦查机关收集通信记录信息的行为,德国刑事诉讼法的规制密度则有所降低,主要表现在两个方面:一是放宽了适用的犯罪案件范围(只要借助电信通信实施了犯罪行为均可纳入适用范围)。二是侦查重大犯罪行为时,对法院命令记载的明确性要求可不必严格遵守。

针对侦查机关截取通信内容信息的行为,美国ECPA作出了比侦查机关调取通信记录信息行为更严格的法律规制,主要表现在三个方面:一是在证据门槛上,截取通信内容信息需要达到具备“相当理由”的程度;而调取通信记录信息的理由只需要达到“有特定及具体事实认为有合理根据证明调取的记录与正在侦查中的犯罪之间具有关联性和实质性时”的程度即可。二是在案件适用范围上,截取通信内容信息只适用于重罪侦查;调取通信记录信息则无此限制。三是在审批程序上,截取通信内容信息需要高级检察官向法官申请,由法官颁发令状才可实施;调取通信记录信息无需高级检察官申请,可依事先通知的传票或经事先通知的法院命令

实施[8]。

然而,值得注意的是,进入数字时代,对侦查机关调取某些能够揭露公民行踪轨迹隐私的通信记录信息的行为,美国联邦最高法院的态度渐趋严厉。在卡彭特案中,联邦检察官根据《存储通信法》向法院申请命令,以获取卡彭特和其他几名同伙的手机基站记录。联邦地方法院核发了两项命令,要求卡彭特的电信运营商公开抢劫案发生的四个月期间,卡彭特手机起始呼叫和结束呼叫的基站记录。依据两份法院命令,警方共获得 12898 个基站位置信息,这些信息记录了卡彭特的移动状况——平均每天 101 个数据。审判前,卡彭特向地方法院提出证据排除动议。他认为,警方调取这些基站记录违反了宪法第四修正案的令状原则和相当理由要求。地方法院驳回了卡彭特的动议,他一路上诉至美国联邦最高法院。

2018 年,美国联邦最高法院判决认为,本案中,警方获取卡彭特手机基站记录的行为,属于宪法第四修正案规定的搜查,但警方仅以法院命令而不是司法令状的方式获取记录有违宪法要求。联邦最高法院的主要理由是:在数字时代,手机基站记录提供了公民更多的隐私信息,这种记录可以让警方随时回溯追踪一个人的行踪轨迹,给警方实施近乎完美的监控(near perfect of surveillance)创造了便利和机会。为遏制这种态势,有必要对这类侦查手段加强法律规制[9]。

(二)传输中的通信内容信息和已存储的通信内容信息

根据信息状态的不同,通信内容信息可以分为传输中的通信内容信息和已存储的通信内容信息。传输中的通信内容信息是指,从通信发起一方发出,尚未到达通信接受一方的通信内容信息。已存储的通信内容信息是指,从通信发起一方发出,已经到达通信接受一方,并存储在相应系统的通信内容信息。一般认为,传输中的通信内容信息涉及典型的通信过程,属于通信自由和通信秘密基本权利的保护范围,而已存储的通信内容信息无关通信过程,属于一般隐私权保护范围[8]。有鉴于此,对于侦查机关收集传输中通信内容信息的行为,法律应当作出比收集已存储通信内容信息的行为更高密度的规制,这在前述美国 ECPA 的立法经验中已经得到体现。

值得关注的是,在数字时代,出现了新的通信形式——网络通话。对于侦查机关收集网络通话中传输的内容信息的行为,一些法治国家倾向于严格规制。所谓网络通话是指,通话参与人借助互联网络,利用 QQ、微信等即时通信软件实施的通话。网络通话的原理不同于传统的非网络通话。网络通话是采用一种去中央化的网际协议通话技术,将语音切割成资料封包,不经中央服务器,而是通过网络自行搜寻最近的路径,传送至受话方,达成语音通话。这种以通话参与人双方为收受源头的“端点对端点”的传输,由于传输过程中使用加密技术,将语音讯号从源头端的发话方即开始编码,透过网络传输到目的端的受话方,再解密还原成信息。由于使用了加密技术,侦查机关无法在电信服务商线路截取到有内容意义的信息,只会取得传输过程中的加密乱码。鉴于网络电话点对点加密传输的特性,侦查机关应在语音信号尚未编码加密前的发话端或已解密后的受话端,安装木马程序记录未加密或已解密的信息内容。

这种新的侦查手法——“来源端电信监察”在德国出现后,引起较大争议。争议的焦点是,能否以刑事诉讼法中规定的传统电信监察条款,作为侦查机关采取该措施的法律授权依据。反对方认为,来源端电信监察虽然是为了监察通信内容,但除了侵犯秘密通信自由外,其干预手段本身——入侵通信者的资讯科技系统安装木马程序——已成为一种对资讯科技基本权的重大干预[10]。为了满足宪法要求,2017 年,德国立法者在修改刑事诉讼法时,在已存在的传统电信监察规定下,新增来源端电信监察条款。该新增条款依附在传统的电信监察条款中,将来源端电信监察当做传统电信监察的补充手段,因此原则上比照传统电信监察应当遵守的法律要件[11]。

不过,通信内容信息毕竟有别于通信记录信息,即使调取已存储的通信内容信息,侦查机关也不能类推适用调取通信记录信息的法律授权依据,否则就有适用法律错误之嫌,这在我国台湾地区的“陈昭全案”中得到了明显体现。

在该案中,被告人陈昭全使用电信服务商提供的 Hibox 服务经营六合彩赌博业务。赌客们以传真送出签注单后,Hibox 会将签注单以电子邮件形式寄送到陈昭全的电子邮箱中。检察官知悉情况后,依据“通讯保障及监察法”向法院申请通信记录调取票获准后,从电信服务商处取得了陈昭全已收受的电子邮件,作为证明被告人犯罪的证据之一。陈昭全主张,检察官取得的签注单是通过违法的方式获取的,无证据能力,应予排除。法院接受了陈昭全

的主张,认为储存于Hibox系统内的传真信息属于被告人的通信隐私,侦查机关必须事先取得法院所核发的通信监察书,才可以调取。本案中,检察官是以调取票取得被告人的电子邮件,违反了“通讯保障及监察法”第5、6条的要求,由此取得的证据应予以排除。检察官不服判决,一路上诉至“最高法院”。“最高法院”判决认为,通信记录指的是电信使用人使用电信服务后,电信系统所产生的发送方、接送方的电信号码、通信时间、使用长度、位址、服务类型、信箱或位置信息等记录。本案中的签注单涉及通信内容,不是通信记录或使用者资料,不能以“通讯保障及监察法”中调取票的规定调取之,而必须要获得法官核发的扣押裁定,方得调取③。

如果已接受的通信内容信息不是存储在第三方,而是存储在自己的手机中,警方不能依据前次逮捕或搜查的授权径直取得嫌疑人手机内的通信内容信息,而是必须获得新的、独立的搜查授权后,方可查看手机内的通信内容信息。在2014年的莱利案中,美国联邦最高法院认为,先例中允许对嫌疑人进行“无证搜查”的理由,并不能适用于针对手机中数据信息的搜查;除非遇到特别紧急的情况,警方若想查看嫌疑人手机中的内容,必须首先取得法院的许可。手机中存储着公民大量的“生活隐私”,因此,存储在手机上的数据也适用宪法中有关隐私保护的条款。即使为打击犯罪,执法部门也不能以牺牲公民隐私利益为代价。警察在对嫌疑人实施逮捕时,如果要搜查嫌疑人手机中的数据,也必须事先获得搜查令状[12]。

二、我国侦查机关收集通信信息的规范现状

目前在我国,侦查机关收集通信信息的措施种类繁多,各类措施所依据的规范性文件的效力等级并不完全相同,有必要对此进行全面的梳理。下面笔者将以规范性文件效力等级为序,从高到低对这些措施进行梳理。如果同等级的规范性文件中,规定了多个可以收集通信信息的措施,则再按照规范密度从高到低进行排列。

(一)以法律作为授权依据的措施

1.技术侦查措施

我国《刑事诉讼法》第150条对技术侦查措施作了特别授权规定。《公安机关办理刑事案件程序规定》(以下简称《程序规定》)第264条将“技术侦查措施”定义为,由设区的市一级以上公安机关负责技术侦查的部门实施的记录监控、行踪监控、通信监控、场所监控等措施。据此,侦查机关采取通信监控类技术侦查措施,收集嫌疑人之间的通话内容信息,有明确的法律授权。刘梅湘教授的实证研究表明,在收集毒品案件、盗窃案件关键证据方面,通信监控类技术侦查措施发挥着一般侦查措施难以替代的作用[13]。例如,在叶某军盗窃案中,采取技术侦查措施决定书、复听技侦内容报告证实,经河南省驻马店市公安局的批准,案件侦办人员对本案涉案人员采取技术侦查手段监听通话录音,从2019年8月27日至8月30日期间,叶某军与刘某通话商量到正阳县作案;叶某军及妻子孙某霞、许某、刘某妻子李某霞之间通话商量案情,如何处理赃物及分赃事宜;叶某军与白某通话商量销赃事宜④。

2.扣押邮件、电报措施

《刑事诉讼法》第143条规定:“侦查人员认为需要扣押犯罪嫌疑人的邮件、电报的时候,经公安机关或者人民检察院批准,即可通知邮电机关将有关的邮件、电报检交扣押。”《程序规定》第232条规定:“扣押犯罪嫌疑人的邮件、电子邮件、电报,应当经县级以上公安机关负责人批准,制作扣押邮件、电报通知书,通知邮电部门或者网络服务单位检交扣押。”根据我国通说,扣押邮件、电报措施干预的是我国宪法规定的通信自由和通信秘密权,通信秘密当然及于通信内容秘密[14]。因此,侦查机关采取扣押邮件、电报措施,可以收集到邮件、电报承载的通信内容信息。例如,在孙某国敲诈勒索案中,上海市公安局水上公安局提交的“扣押邮件/电报通知书”“扣押物品、文件清单”“工作情况”及扣押的敲诈勒索信件证实,案件侦办人员于2017年12月26日,从湖北省武汉市余家头邮局、钢花新村邮局以及杨春湖邮局等5个邮局,扣押了被告人孙某国寄出的133封敲诈勒索信件⑤。

3.调取证据措施

《刑事诉讼法》第54条规定:“人民法院、人民检察院和公安机关有权向有关单位和个人收集、调取证据。有关单位和个人应当如实提供证据。”《程序规定》第62条规定:“公安机关向有关单位和个人调取证据,应当经办案部门负责人批准,开具调取证据通知书,明确调取的证据和提供时限。”尽管在我国,有学者认为从性质而言,调取证据规定是一个概括授权的规定,只能作为侦查机关采取轻微干预措施的法律授权依据,不能作为采取干预基本权利,

如通信自由和通信秘密权措施的法律授权依据[15],但由于上述规定用语较为模糊,含义不够明确,在实践中,侦查机关依据上述规定收集通信信息,已成侦查惯例。例如,吴某某盗窃案中,《调取证据通知书》及通话记录证实,案件侦办人员调取了吴某某手机186××××8609及166××××3249于2020年7月至8月的通话记录,其中号码为166××××3249的手机,在2020年7月1日、2日、14日,8月1日至11日期间多次通话中,显示的通话地在贵州省都匀市⑥。

(二)以其他规范性文件作为授权依据的措施

1.网络远程勘验

最高人民法院、最高人民检察院、公安部制定的《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》(以下简称《电子数据规定》)第9条第3款规定:"为进一步查明有关情况,必要时,可以对远程计算机信息系统进行网络远程勘验。进行网络远程勘验,需要采取技术侦查措施的,应当依法经过严格的批准手续。"一般认为,网络远程勘验的对象是远程计算机信息系统存储的各种电子数据信息[16]。这些电子数据信息当然包含以数字化形式存在的通信信息。因此,侦查机关可以采取网络远程勘验措施,收集存储在远程计算机信息系统内的通信信息。例如,在舒某扰乱国家机关工作秩序案中,网络远程勘验记录证实,舒某通过其网易邮箱发送控告材料⑦。

2.网络在线提取

《电子数据规定》第9条第2款规定:"对于原始存储介质位于境外或者远程计算机信息系统上的电子数据,可以通过网络在线提取。"网络在线提取和网络远程勘验的区别主要有两点:一是针对的对象有所不同。网络在线提取针对的对象,主要是远程计算机信息系统中以公开形式存在的电子数据。网络远程勘验措施针对的对象,主要是远程计算机信息系统中以隐蔽形式存在的电子数据,如被毁灭的电子数据、设有保密措施的电子数据等。二是网络在线提取对远程计算机信息系统不具有侵入性,网络远程勘验则对远程计算机信息系统具有侵入性。例如在深圳市昊某某电子科技有限公司、陈某宁等走私普通货物、物品案中,网络在线提取笔录显示,案件侦办人员依法对卓盟公司企业邮箱85个账号邮箱内的内容提取并固定⑧。

3.电子数据检查

《电子数据规定》第16条第1款规定:"对扣押的原始存储介质或者提取的电子数据,可以通过恢复、破解、统计、关联、比对等方式进行检查。必要时,可以进行侦查实验。"一般认为,电子数据检查是一个相对独立的侦查措施。电子数据检查是处于电子数据收集与电子数据鉴定之间的中间环节,该措施可以进入存储介质虚拟空间内部进行内容上的检索[17]。因此,侦查机关可以采取电子数据检查措施,恢复犯罪嫌疑人删除的通信内容信息。例如在徐某敏非法制造、买卖、运输、邮寄、储存枪支、弹药、爆炸物罪案中,公安司法鉴定中心对徐某敏的手机数据进行恢复,数据显示有"冷月"与"AA…隆达商贸"买卖气枪枪支的聊天记录、转账记录,"AA…隆达商贸"与"沉寂的岁月"买卖枪支的聊天记录、微信转账记录,以及"AA…隆达商贸"与"小胡子"买卖枪支的微信聊天记录、微信转账记录等⑨。

三、侦查机关收集通信信息法律规制存在的问题

从以上梳理可见,我国已经初步形成了规制侦查机关收集通信信息的法律体系。但如果仔细检视这一体系,可以发现,其中仍然存在着诸多不足,下面我们择其要者论之。

(一)某些措施的授权依据和程序不符合宪法要求

我国《宪法》第40条规定:"中华人民共和国公民的通信自由和通信秘密受法律的保护。除因国家安全或者追查刑事犯罪的需要,由公安机关或者检察机关依照法律规定的程序对通信进行检查外,任何组织或者个人不得以任何理由侵犯公民的通信自由和通信秘密。"这一规定在宪法理论上属于"完全宪法保留"。"完全宪法保留"是指,干预某项基本权利的全部领域须遵循宪法的限制条件。《宪法》第40条属于"完全宪法保留",宪法对此设置了主体(限于公安机关或检察机关)、条件(因国家安全或者追查刑事犯罪的需要)和程序(依照法律规定的程序)等三重限制,构造了严密的保护之网[18]。

但上述列举的,具有收集通信信息作用、干预公民通信自由和通信秘密基本权利的网络远程勘验、网络在线提取和电子数据检查措施,其授权依据和程序却来源于司法解释,明显违背《宪法》第40条规定的"依照法律规定的程序"的要求。"无论是现场提取还是网络在线提取,《电子数据规定》并未规定其审批程序。而诸如E-mail之类电子数据承载

了公民通信自由权，侦查人员无需经过审批程序就可以通过网络在线提取收集通信类电子数据，在内容上显然违背了《宪法》第40条所要求的遵循‘法律规定的程序’之规定。”[19]

（二）对某些措施的规制不符合比例原则

根据比例原则要求，国家权力干预行为的严重性应当与法律规制的严格性成比例。也就是说，干预行为的侵权程度越高，越应当受到法律的严格规制。域外法治国家和地区在规制侦查机关收集通信信息的措施时，基本上遵循了这一原理。由于收集传输中的通信内容信息侵权程度最高，法治国家和地区对此均采取了最严格的规制态度，次之是收集已存储的通信内容信息，最后是收集已存储的通信记录信息。

反观我国现有的规制体系，却存在有违比例原则要求之嫌。例如，《程序规定》将通信监控和记录监控统一纳入技术侦查措施中，科以同样的规制密度。但是，通信监控属于收集传输中通信内容信息的措施，侵权程度最高，而记录监控属于收集已存储通信记录信息的措施，与前者相比，侵权程度明显减弱，《程序规定》将二者科以同样的规制密度，明显有违比例原则。又如，在德国，网络远程勘验措施因同时侵犯秘密通信自由和资讯科技基本权，而受到刑事诉讼法最严格的规制。但在我国，网络远程勘验措施受到的法律规制却异常宽松，不仅规制的文件效力等级相对较低，而且欠缺任何实质性的规制要件，与比例原则的要求背道而驰。

（三）没有明确收集手机基站记录信息行为的性质

手机基站记录信息不同于一般的通信记录信息，收集、分析手机基站记录信息能清晰反映出犯罪嫌疑人的行踪轨迹，对实现侦查目的具有重要价值。侦查机关收集手机基站记录信息的行为是否属于技术侦查措施中的通信监控类措施，有解释的空间。从属性上看，手机基站记录信息属于广义的通信信息，似乎属于通信监控干预的对象。但在现代汉语中，“监控”一词针对的是动态发展变化的对象，不适用于静止不变的对象。手机基站记录信息是一种静止不变的记录信息，不应成为通信监控的对象。技术侦查措施中虽然也规定了记录监控类措施，但《刑事诉讼法》和《程序规定》中并未明确手机基站记录信息是否属于记录监控类措施针对的对象。

鉴于技术侦查措施的内涵较为模糊，且适用技术侦查措施的程序相对严格，在实践中，侦查机关倾向于用规制最宽松的调取证据措施来收集手机基站记录信息，但是，这种做法的法律依据并不充分，往往引发被告人和辩护律师的质疑。

（四）扣押邮件、电报措施的规制密度较低

我国刑事诉讼法规定的采用扣押邮件、电报措施收集传输中的通信内容信息，存在直接侵害公民的通信自由和通信秘密权的可能。侦查机关采取这项措施时，理应接受较为严格的法律规制。但我们检视现有法律条文可知，实际的规制密度却较低。首先，措施启动欠缺客观的证据门槛。只要侦查人员认为需要，即可采取该措施，启动门槛较低。其次，审批门槛较低。《刑事诉讼法》笼统地规定“经公安机关或者人民检察院批准”，《程序规定》虽然明确规定“应当经县级以上公安机关负责人批准”，但对比同属于收集传输中通信内容信息的通信监控类技术侦查措施，需要“设区的市一级以上公安机关负责人批准”这一审批门槛明显偏低。最后，措施内容不够完善。相关法律法规对于这一措施的规定未能比照通信监控类技术侦查措施，没有规定执行的期限，未对侦查人员科以保密义务。

（五）未建立符合《个人信息保护法》要求的相应机制

我国《个人信息保护法》第17条规定：“个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项：（一）个人信息处理者的名称或者姓名和联系方式；（二）个人信息的处理目的、处理方式，处理的个人信息种类、保存期限；（三）个人行使本法规定权利的方式和程序；（四）法律、行政法规规定应当告知的其他事项。”侦查机关收集通信信息的行为属于《个人信息保护法》意义上的“处理个人信息”，但现行《刑事诉讼法》却未充分遵循个人信息保护法的要求，建立相应的信息处理告知机制。

在比较法的层面，虽然众多的收集通信信息的行为属于秘密侦查行为，但此处的秘密仅指措施启动和实施过程中收集的秘密，措施结束后，侦查机关仍应向当事人告知信息处理事项。例如，德国《刑事诉讼法》第101条第5项规定：一旦不危及侦查目的、他人的生命、身体之不受侵犯权与人身自由，以及重要财产价值时，第110a条情形中还包括不危及继续任用该卧底侦查员的可能性，即视作通知。如果第一句的通知被延缓，理由应当记入案卷。美国ECPA也规定，侦查机关依据该法律收集通信信息时，原则上应通知信息被收集之人，只有法院认为，

通知将造成对他人生命或身体危险、逃亡、伪造或变造证据、威胁或恐吓证人,或是严重危害侦查或审判迟延者,得签发命令,暂时不予通知。

《个人信息保护法》第47条规定:“有下列情形之一的,个人信息处理者应当主动删除个人信息;个人信息处理者未删除的,个人有权请求删除:(一)处理目的已实现、无法实现或者为实现处理目的不再必要;(二)个人信息处理者停止提供产品或者服务,或者保存期限已届满;(三)个人撤回同意;(四)个人信息处理者违反法律、行政法规或者违反约定处理个人信息;(五)法律、行政法规规定的其他情形。”检视我国《刑事诉讼法》和相关规范性文件,其中并没有建立主动删除通信信息的机制。《刑事诉讼法》第152条第2款仅规定,对采取技术侦查措施获取的与案件无关的材料,必须及时销毁。换言之,与案件有关的材料,并不在主动删除、销毁之列。因此,该规定距离《个人信息保护法》所要求的主动删除机制仍有差距。

四、侦查机关收集通信信息法律规制的完善

我国《宪法》对干预公民通信自由和通信秘密权采取了“完全宪法保留”方式,《个人信息保护法》也将含有行踪轨迹信息的通信记录信息列为敏感个人信息,要求重点保护。在此背景下,有必要正视现行法律规制存在的不足,加强对侦查机关收集通信信息的法律规制。

(一)赋予某些新型措施法律特别授权依据,以符合宪法要求

习近平总书记指出:“依法治国,首先是依宪治国;依法执政,关键是依宪执政。”党的十八大以来,以习近平同志为核心的党中央坚持依宪治国、依宪执政,将全面贯彻实施宪法作为全面依法治国、建设社会主义法治国家的首要任务和基础性工作,把党和国家各项事业、各项工作全面纳入宪法轨道,坚决维护宪法法律权威。在此背景下,某些由司法解释创设的具有收集通信信息功能的新型侦查措施,面临着合宪性危机,这在客观上有违依宪治国、依宪执政的要求。

为消除这一危机,可以将《电子数据规定》创设的网络远程勘验、网络在线提取和电子数据检查三种措施纳入刑事诉讼法规制,由刑事诉讼法赋予这些侦查措施特别授权依据,规定具体的执行程序,以符合宪法要求。笔者认为,目前比较可行的完善方案有以下两种。

第一,在《刑事诉讼法》“侦查”一章中增加一节“电子数据的收集与提取”,对网络远程勘验、网络在线提取和电子数据检查三种措施作出特别授权规定。同时,鉴于三种措施的干预性有别,应当进一步制定差异化的规制程序。对权利干预性最强的网络远程勘验,应当进行最严格的法律规制,分别从证据门槛、适用的案件范围、具体的审批程序、应当承担的保密义务等方面进行高密度的法律规制。对权利干预性次之的网络在线提取和电子数据检查措施,也应当进行一定密度的法律规制。

第二,依据《刑事诉讼法》“侦查”一章的现行体系,将网络远程勘验、网络在线提取和电子数据检查三种措施纳入不同的侦查行为中予以规范。网络远程勘验的权利干预性最强,可以将其纳入技术侦查措施中,作为技术侦查措施的一个具体类型进行规制。将网络在线提取纳入搜查措施中,作为搜查措施的一种具体类型进行规制。将电子数据检查纳入勘验、检查措施中,作为勘验、检查措施的一种具体类型进行规制。

(二)以比例原则为指导进行相应密度的法律规制

前文已指出,按照信息性质的不同,可以将通信信息区分为通信内容信息和通信记录信息;按照信息状态的不同,可以将通信内容信息区分为传输中的通信内容信息和已存储的通信记录信息。侦查机关收集传输中的通信内容信息直接干预公民通信自由和通信秘密权,应当接受最严格的法律规制。侦查机关收集已存储的通信记录信息,虽然也干预公民通信秘密权,但干预程度有所减弱,可以对其作次一级的法律规制。观诸域外法治国家或地区的规制经验,均是以上述规制原理来指导立法实践。

然而,我国《刑事诉讼法》关于技术侦查措施的现行立法却与上述规制原理存在一定程度的背离,不完全契合比例原则的要求。笔者认为,当前比较可行的改进方案是,对干预性最强的通信监控类技术侦查措施和网络远程勘验措施作最高密度的法律规制;对干预性次之的记录监控类、行踪监控类和场所监控类技术侦查措施作次级密度的法律规制,放宽案件适用范围、审批手续的要求。因为在数字时代,如记录监控这类措施,已经广泛应用于各类案件侦查中,如果仍然将这类措施的运用范围局限于“危害国家安全犯罪、恐怖活动犯罪、黑社会性质的

组织犯罪、重大毒品犯罪或者其他严重危害社会的犯罪案件”，无异于“自废武功”，影响侦查机关打击犯罪的能力。

此外，需要明确的是，收集、分析手机基站记录信息能够清晰地反映出嫌疑人的行踪轨迹，因此，应将其归属于记录监控类技术侦查措施，适用较严格的法律规制，侦查机关不能采取调取证据措施径直调取相关人的手机基站记录信息。在我国，《刑事诉讼法》第54条规定的调取证据规定，只是一个侦查概括授权规定，其只能作为侦查机关调取一般公共信息，采取干预性较轻微的侦查措施的法律授权依据，不能作为调取敏感个人信息等干预性较严重的侦查措施的法律授权依据[20]。

（三）大幅度提升扣押邮件、电报措施的法律规制密度

刑事诉讼法作为宪法的“测震仪”，其制定内容必须符合宪法的精神和要求。我国宪法在制定时，采取“完全宪法保留”的形式，高度重视保障公民的通信自由和通信秘密权。与这一情相形对应，在规制干预公民通信自由和通信秘密权的侦查措施时，刑事诉讼法应当采取较为严格的规制态度，贯彻宪法的精神和要求。

扣押邮件、电报措施直接干预公民通信自由和通信秘密权，但目前在我国刑事诉讼法中的规制密度却比较低，有必要大幅度提升该措施的规制密度。基本的思路是，比照通信监控类技术侦查措施来设置扣押邮件、电报措施规制的密度，因为二者都直接干预公民通信自由和通信秘密权。笔者认为，当前应进行以下具体的规制：一是设立措施发动的证据门槛，侦查机关必须在“立案后”才可以采取扣押邮件、电报措施。二是提升审批门槛，采取该措施应由“设区的市一级以上公安机关负责人批准”。三是规定每次扣押的期限为三个月，需要继续扣押时，必须再呈请审批。四是对侦查人员科以保密的义务。

（四）扣押嫌疑人手机后如需查看通信内容信息，需要独立授权

在数字时代，随着智能手机的发展，手机中储存的个人隐私越来越多。根据手机短信、微信、淘宝等程序，几乎可以“重构”手机使用者过去几个月甚至几年的生活。可以说，手机储存信息是个人隐私最集中的地方之一，甚至可能比其住宅中包含的隐私信息更多、更丰富。实践中，我国侦查人员往往在执行搜查、扣押嫌疑人手机措施时，径直查看存储的手机通信内容，甚至直接使用该手机进行“钓鱼”通信。

笔者认为，有必要对这种侦查行为加强法律规制。原因在于，侦查人员搜查、扣押嫌疑人手机时得到的授权，主要是为了控制犯罪嫌疑人的财产、提取和保存证据，这种授权的控制范围仅局限于财产权的范围。扣押嫌疑人手机后，侦查人员查看手机通信内容信息的行为，或者使用该手机进行“钓鱼”通信的行为，干预的是嫌疑人的通信自由和通信秘密权或者一般的隐私权，这已经超越财产权的范围。因此，这种查看行为事实上已经构成一次独立的干预，需要得到独立授权。在2014年的莱利案中，美国联邦最高法院就认为，除非遇到特别紧急的情况，警方若想查看嫌疑人手机中的内容，必须首先取得法院的许可。我国刑事诉讼法也应当作出类似规定，只有在紧急情况下，侦查人员搜查、扣押嫌疑人手机后，才可以径直查看存储在手机内的通信内容；如无紧急情况，侦查人员查看嫌疑人手机通信内容，应当申请独立的授权。

（五）建立符合《个人信息保护法》要求的相应保护机制

为保护个人信息权益，《个人信息保护法》推出了诸多新机制，这些新机制也应引入侦查领域，提升侦查机关处理个人信息的法治化水平。

第一，建立个人信息处理告知机制。在侦查领域，收集通信信息的侦查措施，既有秘密运用的技术侦查措施，也有公开使用的扣押邮件、电报措施。可以结合措施运用的不同形态，建立相应的告知机制。对于秘密使用的技术侦查措施，侦查机关应在措施结束后，在不危及侦查目的及其他正当目的的情况下，主动将收集通信信息的情形告知当事人。对于公开使用的扣押邮件、电报措施，侦查机关应在措施采取前，在不危及侦查目的及其他正当目的的情况下，将准备收集通信信息的情形告知当事人。这种情况类似于公开搜查措施的运用。在采取公开搜查措施前，侦查机关实际上也已经履行了相关的告知义务。

第二，建立主动删除机制。在处理目的已经实现或不再必要时，侦查机关应主动删除收集的通信信息。在侦查机关未主动删除的情形下，应赋予个人删除侦查机关收集的个人通信信息的请求权，并且应当将删除的过程记入侦查案卷之中。

注释

①参见黑龙江省建三江农垦法院（2015）建刑初字第42号判决书，

黑龙江省农垦中级人民法院(2015)垦刑终字第55号裁定书。②“电信通信记录”判决,参见台湾地区司法机构大法官书记处:《德国联邦宪法法院裁判选辑》(十一),台湾地区司法机构印行,2004年,第256页。③参见我国台湾地区“最高法院”2016年度台非字第259号判决。④参见河南省正阳县人民法院刑事判决书(2022)豫1724刑初247号。⑤参见上海市虹口区人民法院刑事判决书(2018)沪0109刑初1009号。⑥参见贵州省都匀市人民法院刑事判决书(2021)黔2701刑初174号。⑦参见四川省遂宁市安居区人民法院刑事判决书(2018)川0904刑初40号。⑧参见广东省深圳市中级人民法院刑事判决书(2021)粤03刑初90号。⑨参见贵州省大方县人民法院刑事判决书(2018)黔0521刑初251号。

参考文献

[1]谢登科.电子数据网络在线提取规则反思与重构[J].东方法学,2020(3):89-100.

[2]陈永生.刑事诉讼中搜查手机的双重司法审查机制[J].北京航空航天大学学报(社会科学版),2022(2):34-37.

[3]中国社会科学院语言研究所词典编辑室.现代汉语词典:第7版[M].北京:商务印书馆,2016:1311.

[4]薛殿杰.利用通信信息痕迹的侦查方法[J].江苏警官学院学报,2004(1):167-173.

[5]张翔.通信权的宪法释义与审查框架[J].比较法研究,2021(1):33-48.

[6]伯阳,刘志军.一般人格权之具体体现:新创设的保障IT系统私密性和完整性的基本权利:联邦宪法法院对“在线搜查”作出的判决[J].中德法学论坛,2008(6):33-50.

[7]林钰雄,王士帆,连孟琦.德国刑事诉讼法注释书[M].台北:新学林出版股份有限公司,2023:174-180.

[8]李荣耕.犯罪侦查中通讯内容的调取[J].台大法学论丛,2022(3):759-831.

[9]艾明.从马赛克理论到完美监控理论:大数据侦查法律规制的理论演进[J].北大法律评论,2022(1):1-20.

[10]林钰雄.侵入资讯科技系统之来源端通讯监察[J].月旦法学教室,2021(5):16-19.

[11]王士帆.当科技侦查骇入语音助理:刑事诉讼准备好了吗?[J].台大法学论丛,2019(6):191-242.

[12]刘广三,李艳霞.美国对手机搜查的法律规制及其对我国的启示:基于莱利和伍瑞案件的分析[J].法律科学,2017(1):180-190.

[13]刘梅湘.监控类技术侦查措施实证研究[J].华东政法大学学报,2019(4):90-101.

[14]郎胜.《中华人民共和国刑事诉讼法》修改与适用[M].北京:新华出版社,2012:266.

[15]艾明.调取证据应该成为一项独立的侦查取证措施吗?[J].证据科学,2016(2):155-166.

[16]谢登科.电子数据网络远程勘验规则反思与重构[J].中国刑事法杂志,2020(1):58-68.

[17]谢小剑,朱春吉.论智能手机中电子数据检查的隐私权保护[J],法治论坛,2020(3):95-109.

[18]秦小建.新通信时代的实践争议与宪法回应[J].政治与法律,2020(7):85-97.

[19]谢登科.论电子数据收集中的权利保障[J].兰州学刊,2020(12):33-45.

[20]艾明.刑事诉讼法中的侦查概括条款[J].法学研究,2017(4):155-172.

On the Legal Regulation of Investigation Agencies Collecting Communication Information in the Digital Era

Ai Ming

Abstract: Although a legal system to regulate the collection of communication information by investigation agencies has been initially established in China, yet it has not been able to respond well to the development trend of the digital age and has many shortcomings. In the digital age, diverse forms of communication information carry different legal interests for protection. Legislators should distinguish between these different protection interests, follow the essential characteristics of communication information types, and make proportional and targeted legal regulations. Specifically, China should strengthen legal regulations in the following aspects: firstly, the Criminal Procedure Law should provide special authorization basis for certain new investigative measures to comply with constitutional requirements; Secondly, according to the different types of communication information, legal regulations of corresponding density should be guided by the principle of proportionality; The third is to significantly increase the legal regulatory density of measures to seize mails and telegrams; The fourth is to independently authorize the behavior of viewing the suspect's mobile communication content information; The fifth is to establish corresponding protection mechanisms that meet the requirements of the Personal Information Protection Law.

Key words: digital age; investigation agencies; communication information; personal information; legal regulation

责任编辑:一　鸣